

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
TARGET DEVICE #1: BLACK IPHONE IN A CASE WITH A PICTURE OF AN ALIEN AND THE PHRASE, "TAKE ME TO YOUR DEALER", SEIZED ON APRIL 16, 2021 FROM KEENAN YOUNG AT 823 WALNUT STREET, APARTMENT 1, PITTSBURGH, PA 15221 (ATTACHMENT A, SECTION 1).	Mag. No. 21-863

APPLICATION/AFFIDAVIT FOR SEARCH WARRANTS

I, Task Force Officer William Churilla, having been duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

Your Affiant, Task Force Office William Churilla, being duly sworn according to law, aver that the following is true and correct to the best of my knowledge, information and belief and is based on personal knowledge or information provided by reliable sources.

Your Affiant is a member of both the Pittsburgh Bureau of Police (PBP) and is also a Task Force Officer with the Drug Enforcement Administration (DEA). As a Pittsburgh police officer, I am empowered under state law to make arrests for violations of state criminal laws, and I am also empowered to execute state search warrants. As a DEA Task Force Officer, I am empowered under federal law to make arrests for violations of federal criminal laws, and I am also empowered to execute federal search warrants.

I have a High School Diploma, as well as a bachelor's degree in criminology and Business Management from Duquesne University. After my 1988 graduation from Duquesne University, I worked for approximately 5 years with juveniles adjudicated of crimes at the Allegheny Academy Juvenile Facility. In 1997, I began to work full-time as a police officer for the City of Pittsburgh. I spent the first several years as a patrol officer in the Zone 2 section of Pittsburgh which encompasses neighborhoods including the Hill District. I remain employed with the PBP and became a Detective in approximately 2007.

In 2013, I was assigned to Narcotics and Vice where I primarily investigated drug and firearm offenses. I have purchased drugs including marijuana, cocaine, heroin and fentanyl in an undercover capacity on many occasions and have been involved as a back-up officer in many undercover purchases by other officers. I have been involved in numerous controlled purchases, of various types of drugs, by cooperating individuals. I have obtained numerous search warrants regarding drug and firearm violations and have been involved in numerous similar search warrants obtained by my fellow police officers.

I have been asked to render an expert opinion on many occasions regarding whether various circumstances show that drugs were possessed for distribution, as opposed to personal use. I have been qualified and testified as a narcotics expert in court more than a dozen times. My relevant trainings include the initial Pittsburgh Police Academy training, as well as the "Top Gun" Narcotics Investigation course, Pennsylvania Electronic Surveillance "A" certification training, ATF "Characteristics of Armed Individuals" training, and interrogation and interview training. My drug and firearm experience come from working not only with many other members of the PBP, but with numerous other local, state and federal investigators including the ATF, FBI

and DEA. I have been involved in over 1000 arrests in my career, many involving guns, drugs or both.

This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. This affidavit is largely based on information obtained from reports of other law enforcement officers, laboratory testing results, and other documents. Based on the probable cause set forth below, your affiant is seeking warrants to authorize searches of the following device:

ITEM TO BE SEARCHED

Target Device #1: Black iPhone in a case with a picture of an alien and the phrase, “take me to your dealer”, seized on April 16, 2021 from Keenan Young at 823 Walnut Street, Apartment 1, Pittsburgh, PA 15221 (Attachment A, Section 1).

PROBABLE CAUSE

1. On April 16, 2021, at approximately 6:00 a.m., members of the Pennsylvania State Police (PSP) SRT team executed a federal search warrant at 823 Walnut Street Apartment 1 Pittsburgh, PA 15221. Keenan YOUNG (“YOUNG”) was the target of the search warrant.
2. Once entry was made into the residence YOUNG was taken into custody and was moved into the living room area of the residence. In the presence of SA Palso, TFO Glavach, and Det. Burdette, YOUNG spontaneously stated that everything in the apartment was his. Ofc. Nesser Mirandize YOUNG at this time. YOUNG indicated he understood his rights and stated he would speak without an attorney present. SA Palso and TFO Glavach asked YOUNG to clarify what all was his in the apartment, at which time YOUNG walked TFO Glavach to the master bedroom and pointed to the vanity and stated that a firearm was in it. YOUNG also stated to TFO Glavach that under the bed was crack cocaine in a pink shoe. TFO Glavach recovered a green KelTec handgun SN# K7L71 with a loaded magazine in the vanity drawer.

3. TFO Glavach also recovered individually wrapped knotted baggies containing crack cocaine from on top of the vanity that was located with a digital scale in the vanity drawer. TFO Glavach also recovered a Black iPhone in in a case with a picture of an alien on it and the phrase, "take me to your dealer", on the bed in the master bedroom.

4. Also found in the master bedroom near the vanity were numerous plastic sandwich bags and "diaper" baggies.

5. Det. Burdette searched under the master bed and found two plastic bags containing large chunks of crack cocaine in pink colored shoes. The Crack cocaine was field tested which was positive for cocaine base.

6. In my 24 years of law enforcement experience, I am aware that it is a common practice for drug and firearm traffickers who desire to insulate themselves from detection by law enforcement agents to utilize multiple telephones and communication devices, fictitious identities, coded communications, and other counter-surveillance techniques in communicating and meeting with their customers, suppliers, couriers, and other conspirators. It is not unusual for drug and firearms traffickers to subscribe some or all their telephones in the names of other real or fictitious people.

7. Moreover, it is now a very common practice for drug traffickers to utilize all communication features of their telephones and communication devices, most notably the voice call and text message features, nearly simultaneously to communicate with their conspirators.

8. For example, it is quite common for a particular transaction to be set up and completed using both voice calls and text messages. In fact, it is now quite unusual for a drug trafficker to utilize solely one feature of a telephone, such as the voice call feature, to further his criminal activities while not also using another feature, such as the text message feature, to further his

criminal activities. Even when a trafficker attempts to do so, he is often not successful because those he communicates with also must similarly limit themselves to utilizing a single cell phone feature and mistakes are often made as a result.

9. I am aware that evidence of drug, firearm, and money laundering crimes can often be found in electronic media, including cellular telephones, laptop computers, cameras, and tablet devices. Such evidence can be found throughout those items, such as in text messages, contact lists indicating the names and numbers of associates, call/text logs indicating calls/text made to and received from associates, online search history files, word processing documents, and photograph and video gallery files. It should be noted that, with the advance of technology, the distinction between computers and cellular telephones is quickly becoming less clear. Actions such as internet searching or emailing, in addition to calling and text messaging and photographing, can now be performed from many cell phones. In addition, as noted above, those involved in drug and firearm trafficking crimes commonly communicate using multiple cellular telephones. Contemporaneous possession of multiple cellular telephones is, therefore, evidence of such trafficking.

10. Moreover, the particular numbers of, and the particular numbers dialed by, particular cellular telephones can be evidence of drug trafficking, particularly in light of the fact that it is a practical necessity that drug traffickers communicate with each other, as well as with their customers and suppliers, by telephone. Such numbers can confirm identities of particular associates and the occurrence of certain events.

11. As with most electronic/digital technology items, communications made from an electronic device, such as a cellular telephone or a standard computer, are often saved or stored on the device. Storing this information can be intentional, for example, by saving a text message or a contact or

an e-mail.

12. Digital information can also be retained unintentionally. Traces of the path of an electronic communication or of an internet search may be automatically stored in many places on a computer or cellular telephone.

13. In addition to electronic communications, a user's internet activities generally leave traces in the web cache and internet history files. A forensic examiner often can recover evidence that shows when and in what manner a user of an electronic device, such as a computer or a cell phone, used such a device. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they often can be recovered months or years later using readily available forensic tools.

14. When a person "deletes" a file on an electronic storage device such as a computer, the data contained in the file often does not actually disappear; rather, that data often remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on a device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten.

15. In addition, a computer's operating system may also keep a record of deleted data in a "swap" "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

16. Thus, the ability to retrieve residue of an electronic file from an electronic storage device depends less on when the file was sent, downloaded, or viewed than on a particular user's operating system, storage capacity, and habits.

17. I am aware that those who illegally possess drugs and guns sometimes take trophy photographs and videos using their cameras and/or cellular telephones of their drugs, firearms, and proceeds and retain them on those devices. In addition, I am aware that drug and firearm traffickers, like law-abiding citizens, sometimes take photographs and videos using their cameras and cellular telephones of themselves with their friends, relatives, and associates and keep the photographs and videos on those devices. When they are taken or retained by drug and firearm traffickers, such photographs and videos can be evidence, and can lead to additional evidence, of illegal trafficking activity by identifying the traffickers, contraband, and people who are actively assisting and/or supporting the trafficking activity as well as the locations where they live or where they store their drugs, firearms, proceeds, or paraphernalia.

18. It should be noted that data on electronic communication and/or storage devices is often relevant to a criminal investigation by revealing who used a particular device. In addition, such data can reveal who resided at or who had access to a particular location if, for example, a particular device was found at a particular location (e.g., inside a particular room of a particular residence) and the device contains data demonstrating that it was used by or belonged to a particular person. In that sense, a particular electronic device can be significant indicia linking a particular person to contraband or another criminal activity even if the device itself does not contain the remnants of incriminating communications.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store

information for long periods of time. Also, internet searches and the correlating data can also be stored on the device. This information can sometimes be recovered with forensic tools.

20. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and pass along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who

used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of Examination.* Based on the foregoing, and consistent with Rule 41(e) (2) (B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of Execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time, whether that be in the day or night.

CONCLUSION

23. Based on the totality of the circumstances surrounding the recovery of the narcotics and the firearm, and your affiant's training and experience in narcotics investigations and the role of cell phones in narcotics trafficking, your affiant believes that there is probable cause to believe that the **Target Device (Target Device #1: Black iPhone in in a case with a picture of an alien on it stating "take me to your dealer"**. Seized on April 16, 2021 from Keenan Young at 823 Walnut Street Apartment 1 Pittsburgh, PA 15221 (Attachment A, Section 1). It will contain evidence of violations Title 21, United States Code, Sections 841(a) (1) and Title 18, United States Code, Sections 922(g) (1) and 924(c).

24. Therefore, I submit this affidavit supporting probable cause for a search warrant authorizing the examination of the Target Devices described in Attachment A to seek the items

described in Attachment B. The above information is true and correct to the best of my knowledge, information, and belief.

/s/ William Churilla
William Churilla,
Task Force Officer
Drug Enforcement Administration

Sworn and subscribed before me, by telephone
Pursuant to Fed. R. Crim. P. 4.1(b) (2) (A),
This 22nd day of April 2021

THE HONORABLE PATRICIA L. DODGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Section 1

The property to be searched is a black iPhone pictured below. The black iPhone is currently being stored at the DEA Headquarters. This warrant authorizes the forensic examination of the black iPhone in in a case with a picture of an alien on it and the phrase, “take me to your dealer”, for the purpose of identifying the electronically stored information.



ATTACHMENT B

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

Records, communications stored at the time the warrant is served (i.e., no real-time communications will be intercepted and searched during service), data, and textual and graphic files (including photographs and videos), evidencing who used the device and when and from where or a violation of Title 18, United States Code, Sections 922 or 924, or Title 21, United States Code, Sections 841 or 846, including:

- (1) Incoming and outgoing call and text message logs;
- (2) Contact lists;
- (3) Photo and video galleries;
- (4) Sent and received text messages;
- (5) Online searches and sites viewed via the internet;
- (6) Online or electronic communications sent and received, including email, chat, and Instant messages;
- (7) Sent and received audio files;
- (8) Navigation, mapping, and GPS files, sim/ sms cards;
- (9) Telephone settings, including speed dial numbers and the telephone number for the Subject telephone and related identifying information such as the ESN for the Telephone;
- (10) call forwarding information;
- (11) Messages drafted but not sent;
- (12) Voice messages;
- (13) Any deleted information from this cell phone.